National Infrastructure Advisory Council (NIAC)

The Insider Threat to Critical Infrastructures

Thomas Noonan
General Manager
IBM Internet Security Systems

Edmund Archuleta
President and CEO
El Paso Water Utilities

Overview

- Objective
- Scope
- Summary: Phase I Study
- Phase II Working Group Activity
- Findings
- Findings and Solutions:
  - Information Sharing
  - Education and Awareness
  - Technology
  - Background Investigations
  - Research
  - Insider Threat Policy
- Next Steps
- Questions

Scope

- Deliverables for the study, as outlined in the January 16 letter from Secretary Chertoff:

  Phase I
  - Define the "insider threat" physical and cyber, including potential consequences, economic or otherwise
  - Analyze the dynamics and scope of the insider threat including critical infrastructure vulnerabilities
  - Analyze the potential impact of globalization on the critical infrastructure marketplace and insider issues
  - Identify/define the obstacles to addressing the insider threat

  Phase II
  - Identify issues, potential problems, and consequences associated with screening employees
  - Identify legal, policy, and procedural barriers aspects of the issue, as well as any potential obstacles, from the perspective of the owners and operators
  - Identify and make policy recommendations on potential remedies for addressing the insider threat (up to and including potential legislation)

Objective

- First Phase focused on defining the insider threat to critical infrastructures, including dynamics involved, obstacles to mitigation, and the effect of globalization
- The second phase of the study has focused on addressing legal, procedural, and policy barriers to private sector infrastructure operator employee screening efforts
- Completion of the study may produce potential recommendations for improving operators' ability to address the insider threat to critical infrastructures, and seek to provide guidance on a clear legal environment for operators in dealing with potentially hostile insiders

Summary: *Phase I* Insider Threat Study

- Held 2 two-day workshops and 25 conference call discussions

Deliverables provided in Phase I draft included:

- Definition for the Insider Threat to CI
- Identified the Scope of the Insider Threat
- Understanding of the Psychology of the Insider Threat
- Understanding of the Technology and Globalization Dynamics
- Outlining the obstacles to effective Insider Threat Programs
  - Information Sharing on insider threats
  - Education and Awareness
  - Background Investigation Processes
  - Technology Tools
  - Cultural and Organizational obstacles

Phase II Working Group Activity

- Elevated work pace since October NIAC meeting
  - Held a two-day workshop and 14 conference call discussions on Phase II topics and report development
  - Discussions with 9 outside subject matter experts (SMEs) to gain understanding of the issues involved
- Developing findings and recommendations for Phase II draft of the report
  - Coordinating Draft Report is near complete
  - Findings and recommendations need final review by the Working Group prior to forwarding to the full NIAC

Findings on the Insider Threat

- Recent studies and events have shown that the Insider Threat is real
  - Many Insider Incidents are unreported to protect corporate image and lack of trusted reporting centers
  - CI/KR companies are under-estimating the risk posed by insider threats
  - Many CI/KR companies are unprotected against some Insider Threat vulnerabilities
  - Unverified trust with employees in positions of significant trust
  - Losses are often magnified by improper incident response
- Insider attacks at CI/KR companies have the potential to cause significant, widespread damage to economic activity and public health
- Growing economic espionage threat has significant potential effect to national security

Insider Threat Policy

CI/KR companies can reduce their insider threat risk by establishing insider threat policies

- Critical infrastructure companies should develop and implement a comprehensive security policy to address internal threats
  - Should be developed and supported by senior executive leadership and include implementation plans and goals

Information Sharing

Lack of information on insider threats has obscured the level of risk involved. Improved information sharing will improve Insider risk assessments and decisions.

1. Establish a mechanism to provide critical infrastructure owner-operator need for timely and relevant strategic-level (intelligence agency) information on insider threats
2. Government should develop a mechanism for sharing information on Insider Threat and National Security investigations, which currently does not exist
3. Each sector should establish a trusted process and protected mechanism to share incident information on insider threats
4. Government should coordinate a clearinghouse resource for owner-operators to assist in the process of assessing and mitigating their insider threat risks

Education and Awareness

Securing our infrastructures will require improvement of CI/KR operator understanding of insider threats.

Education and awareness offers the biggest return for critical infrastructure owner-operators in addressing insider threats.

1. Establish leadership program on insider threats to coordinate government support to CI/KR operators on education and awareness of insider threats
2. Program goals will include development of a common baseline understanding of the emerging and dynamic insider threat issues and situations among CI/KR companies
   - Work directly with critical infrastructure executive leaders
   - Communicate enterprise-level risks posed by insider threats
   - Partner with leading companies in each sector
   - Assist development of education and training programs
   - Identify and fund needed research

Background Investigations

To improve CI/KR operator risk assessment and mitigation for high-trust, critical positions, CI/KR operators need access to Federal and state criminal history records

1. Adopt needed measures from April 2006 Attorney General's Report Criminal History Record Checks
2. Measures should include consideration of CI/KR operator needs and concerns:
   - Voluntary participation
   - CI/KR operators should make their own risk decisions
   - Third party screening company participation
   - Improved records accuracy and standardization
   - Near-term solution

Technology

Technology trends are accelerating and combining with globalization forces, creating significant insider security challenges for CI/KR operators.

Virtual aspect of network environments also poses challenges for establishing accountability and ethical behavior.

- Steering group of IT technology experts to explore insider threat technology solutions
- Improve CI worker IT/network ethics, accountability, and understanding of appropriate conduct on critical infrastructure IT networks, down through university levels
- CI companies should establish priority to maintain current network/IT security best practices

Next Steps

- Coordinate initial findings with Federal Agencies and Privacy groups
- Publish Coordinating draft for Working Group prior April's meeting, then a revised copy to the full NIAC
- Deliver final findings for deliberation at the April 2008 NIAC meeting

Questions?